PROCEDURE 1410.88
Issue Date: April 30, 2006
Effective Date: May 31, 2006

SUBJECT: **Desktop Log-Off / System Shut down**

APPLICATION: Executive Branch Departments, sub-units, and non-executive branch entities using Department of Information Technology managed computer resources.

PURPOSE: Implementation of this standard will provide for streamlines asset management processes, protect the State's networks and internal host systems, reduce internal security risk, and reduce electric utility charges.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: To provide the opportunity for systems audit, asset inventory, verification of configuration, automated download of upgrades, system hot fixes and virus protection updates, and to comply with Executive Directive No. 2003- 10, this procedure defines a requirement to turn off all networked desktop and notebook computing devices at the end of the work day whenever possible and requires log-off and system shut down at least once each week for perpetual use systems.

APPLICABLE FORMS: None

PROCEDURE: This baseline practices is necessary to enhance security, maintain audit, and monitor the desktop computing devices of all State of Michigan networked personal computers.

SCOPE

This policy applies to all DIT owned or managed computer systems. Unless otherwise indicated, the term "user" here refers to employees, student interns, volunteers, and contractors or anyone using state computer systems or network resources.

REQUIREMENTS

DIT is responsible for maintaining practices that enhance the security of statewide data and information technology resources. A necessary practice for all agencies, board, and commission employee users with access to these resources is for all users to log onto and off of computer systems and power down each day when not in use and thereby prohibit unauthorized users from using other users' accounts. A minimum requirement is to power down all desktop systems connected to the State of Michigan's networks at least once each week to facilitate remote services and maintenance. Where available, an automated method may be used to execute this policy.

GUIDELINES

Computers dedicated for use by a single employee user, at the end of each workday the user should power off the computer to prevent unauthorized access. Users who plan to leave the computers unattended for a few minutes or longer should log off network-accessible resources or use password-protected screen savers or sleep modes to prevent unauthorized access during the workday.

For a computer shared by multiple employee end-users, each user should disconnect from network-accessible resources, log-off the computer, and make it available for another user immediately upon completion of his/her "computer session." Users of shared computer systems should not leave their computer sessions unattended and instead log-off if they must leave the immediate vicinity of the computer, then log in again upon return.

Exception Process:
For those desktop computer resources used by multiple shifts or left on because they serve a critical 24x7 business function the following exception process must be followed:

- An Agency Business owner for each computer resource(s) must be identified and provided to the DIT CSD or DIT designee.
- A list of the computers requiring exception to the policy must be provided by the Agency Business Owner to the DIT CSD or DIT designee. The list must include the workstation name, MAC address and location for each computer requiring an exception.
- The Agency Business owner must coordinate with the DIT CSD or DIT designee a schedule whereby the computers are shut-down, to avoid an automated shutdown.

***